Введение в дискретную математику. Лекция 3 (соответствия, функции и бинарные отношения, отношения эквивалентности, кольца $\mathbb{Z}_n$). План-конспект

Н. Л. Поляков

1 Операции над бинарными отношениями (продолжение)

Транзитивное замыкание. Для каждого бинарного отношения $P \subseteq X \times X$ следующим образом определяется *транзитивное замыкание* отношения P:

$$P^* = \bigcup \{P^n : n \in \mathbb{N}\}.$$

Здесь P^n обозначает отношение $\underbrace{P \circ P \circ \ldots \circ P}_{n \text{ раз}}$.

Пример. Пусть P есть отношение на множестве $\mathbb{N}$ натуральных чисел,

$$x \, P \, y \Leftrightarrow y = x + 1.$$

Тогда $P^* = <$.

2 Типы соответствий и бинарных отношений

Типы соответствий. Соответствие R из множества X в множество Y называется

- *всюду определенным*, если

  $$(\forall x \in X)(\exists y \in Y)\,(x, y) \in R,$$

  эквивалентно $R^{-1}(Y) = X$,

- *функциональным* (или просто *функцией*), если

  $$(\forall x \in X)(\forall y, z \in Y)\,((x, y) \in R \wedge (x, z) \in R) \to y = z,$$

  эквивалентно, $R^{-1} \circ R \subseteq E_Y$,

- *сюръективным*, если

  $$(\forall y \in Y)(\exists x \in X)\,(x, y) \in \mathcal{R},$$

  эквивалентно, $R(X) = Y$,

- *инъективным*, если

  $$\forall x, z \in X)(\forall y \in Y)\,((x, y) \in \mathcal{R} \wedge (z, y) \in \mathcal{R}) \to x = z,$$

  эквивалентно, $R \circ R^{-1} \subseteq E_X$.

В классической математике функции (отображения) f из множества X в множество Y отождествляются со всюду определенными функциональными соответствиями из множества X в множество Y, которые в «естественном понимании» можно понимать как *графики* функций. Запись $f : X \to Y$

обозначает, что f есть функция из множества X в множество Y. Символ $f(x)$ обозначает тот единственный для элемента x элемент y, для которого $(x, y) \in f$. Запись $f(x) = y$ используется вместо $(x, y) \in f$. Множество всех функций из множества X множество Y обозначается символом Y^X.

Инъективная и сюръективная функция, т.е. соответствие, обладающее всеми четырьмя указанными выше свойствами, называется *биекцией* (или *биективной* функцией или *биективным* соответствием, или *взаимнооднозначной* функцией/*взаимнооднозначным* соответствием).

Типы бинарных отношений. Бинарное отношение P на множестве X называется

- *рефлексивным*, если $(\forall x \in X)(x\,P\,x)$, равносильно, $E_X \subseteq P$,
- *иррефлексивным*, если $(\forall x \in X)(\neg x\,P\,x)$, равносильно $E_X \cap P = \varnothing$,
- *симметричным*, если выполнено $(\forall x, y \in X)(x\,P\,y \to y\,P\,x)$, равносильно, $P^{-1} = P$,
- *(нестрого) антисимметричным*, если $(\forall x, y \in X)((x\,P\,y \wedge y\,P\,x) \to x = y)$, равносильно, $P \cap P^{-1} \subseteq E_X$,
- *асимметричным*, если $(\forall x, y \in X)(\neg(x\,P\,y \wedge y\,P\,x))$, равносильно, $P \cap P^{-1} = \varnothing$,
- *полным*, если $(\forall x, y \in X)(x\,P\,y \vee y\,P\,x)$, равносильно, $P \cup P^{-1} = X \times X$,
- *связным*, если $(\forall x, y \in X)(x\,P\,y \vee y\,P\,x \vee x = y)$, равносильно, $P \cup P^{-1} \cup E_X = X \times X$,
- *транзитивным*, если $(\forall x, y, z \in X)((x\,P\,y \wedge y\,P\,z) \to x\,P\,z)$, равносильно, $P \circ P \subseteq P$, равносильно, $P^* = P$.

Иррефлексивные отношения называют еще *антирефлексивными*, а асимметричные – *строго антисимметричными*.

Бинарное отношение P на множестве X называется отношением

- *строгого частичного порядка*, если оно транзитивно и асимметрично (следовательно, иррефлексивно),
- *нестрогого частичного порядка*, если оно транзитивно, рефлексивно и антисимметрично,
- *строгого/нестрогого линейного порядка*, если есть отношение строгого/нестрогого частичного порядка и при этом связно,
- *эквивалентности*, если оно транзитивно, симметрично и рефлексивно.

3 Отношения эквивалентности

Отношения эквивалентности и разбиения. Отношения эквивалентности тесно связаны с разбиениями множеств. *Разбиением* множества X (на непустые подмножества) называется любое подмножество $\mathbb{W}$ множества $\mathscr{P}(X) \setminus \{\varnothing\}$, которое обладает следующими свойствами:

1. $\bigcup \mathbb{W} = X$
2. $(\forall U, V \in \mathbb{W})(U \cap V \neq \varnothing \to U = V)$.

Утверждение. Пусть даны множество X и разбиение $\mathbb{W}$ множества X. Тогда следующее отношение P на множестве X

$$x \, P \, y \leftrightarrow (\exists U \in \mathbb{W})(x \in U \wedge y \in U)$$

есть отношение эквивалентности.

Доказательство. Действительно, рефлексивность и симметричность этого отношения очевидны. Транзитивность следует из пункта 2 определения разбиения. Если элементы x и y принадлежат одному и тому же элементу разбиения U, а y и z принадлежат одному и тому же элементу разбиения V, то $y \in U \cap V$, следовательно, пересечение множеств U и V не пусто, и они совпадают. Поэтому элементы x и z принадлежат одному и тому же элементу $U = V$ разбиения $\mathbb{W}$.

Оказывается, любое отношение эквивалентности можно построить таким образом.

Пусть P есть отношение эквивалентности на множестве X.

Для каждого элемента $x \in X$ символом $[x]_P$ обозначается его класс эквивалентности, т.е. множество $\{y \in X \colon x \, P \, y\}$ всех элементов множества Y, которые эквивалентны элементу x. Если речь идет о каком-либо фиксированном отношении эквивалентности, нижний индекс $\mathcal{P}$, как правило, опускают, т.е. пишут просто $[x]$ вместо $[x]_{\mathcal{P}}$.

Утверждение. Для каждого отношения эквивалентности P на множестве X множество всех различных классов эквивалентности $[x]_P$ элементов множества X есть разбиение множества X. Отношение эквивалентности, построенное по этому разбиению так, как в предыдущем утверждении, совпадает с отношением P.

Доказательство. Действительно, в силу рефлексивности отношения P для каждого $x \in X$ имеет место утверждение $x \in [x]_P$. Поэтому $X \subseteq$

$\bigcup\limits_{x\in X}[x]_P$. Обратное включение очевидно. Таким образом, $X = \bigcup\limits_{x\in X}[x]_P$.

Пусть для некоторых элементов $x, y \in X$ множества $[x]_P$ и $[y]_P$ имеют непустое пересечение. Выберем элемент $z \in [x]_P \cap [y]_P$. В силу симметричности отношения P имеем $x\,P\,z \wedge z\,P\,y$. По транзитивности получаем $x\,P\,y$.

Выберем произвольный элемент $y' \in [y]_P$. Тогда $y\,P\,y'$. По транзитивности получаем $x\,P\,y'$, откуда $y' \in [x]_P$. В силу произвольности выбора элемента y' получаем $[y]_P \subseteq [x]_P$. Обратное включение доказывается так же.

Фактор-множество. Множество X/P всех классов эквивалентности $[x]_P$ элементов множества X называют *фактор-множеством* множества X по отношению эквивалентности P. Фактор-множество X/P есть разбиение множества X, причем отношение эквивалентности $P_{X/P}$, построенное по этому разбиению совпадает с исходным отношением P. Таким образом, существует взаимно-однозначное соответствие между всеми отношениями эквивалентности на множестве X и всеми разбиениями множества X.

Отношения эквивалентности и функции. Отношения эквивалентности на множестве X связаны и с функциями из множества X. Действительно,

- для любой функции $f : X \to Y$ отношение $P \subseteq X \times X$, заданное формулой
$$x\,P\,y \Leftrightarrow f(x) = f(y)$$
есть отношение эквивалентности;
- для любого отношения эквивалентности $P \subseteq X \times X$ определим функцию $f_P : X \to X/P$, которая каждому элементу $x \in X$ ставит в соответствие его класс эквивалентности $[x]_P$. Тогда
$$x\,P\,y \Leftrightarrow f_P(x) = f_P(y).$$

Отношения эквивалентности, согласованные с операциями (конгруэнции). Отношение эквивалентности P на множестве X *согласовано* с функцией $f : X^n \to X$, если для всех $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in X$ выполнено

$$x_1\,P\,y_1 \wedge x_2\,P\,y_2 \wedge \ldots \wedge x_n\,P\,y_n \Rightarrow f(x_1, x_2, \ldots, x_n)\,P\,f(y_1, y_2, \ldots, y_n).$$

Множество X, рассматриваемое вместе с некоторым набором функций на этом множестве (от произвольного количества переменных каждая) часто называют *алгеброй*. Отношение эквивалентности на множестве X, согласованное со всеми функциями алгебры $\mathcal{A}$, называется *конгруэнцией* этой алгебры. С помощью конгруэнции P все функции алгебры $\mathcal{A}$ можно перенести на фактор-множество X/P по правилу

$$f\left([x_1]_P, [x_2]_P, \ldots, [x_n]_P\right) = [f(x_1, x_2, \ldots, x_n)]_P.$$

4 Кольца $\mathbb{Z}_n$: для самостоятельного изучения

Кольца $\mathbb{Z}_n$ (см. ниже) являются классическим примером описанной математической конструкции. Кроме того, они представляют самостоятельный интерес. Операции в кольцах $\mathbb{Z}_n$ («модульная арифметика») широко используется как внутри математики, так и в ее приложениях (криптография).

Пусть n – некоторое положительное натуральное число. Рассмотрим следующее отношение $\equiv$ на множестве целых чисел $\mathbb{Z}$:

$$x \equiv y \leftrightarrow (x - y) \text{ делится на } n,$$

т.е.

$$x \equiv y \leftrightarrow (\exists k \in \mathbb{Z})(x - y = kn).$$

Покажем, что это отношение эквивалентности. Действительно,

- $\forall x(x - x = 0 \cdot n)$, следовательно, отношение $\equiv$ рефлексивно;
- $\forall x, y(x - y = k \cdot n \to y - x = (-k) \cdot n)$, следовательно, отношение $\equiv$ симметрично;
- пусть для произвольных целых чисел x и y существуют такие целые числа k_1 и k_2, что

  $$x - y = k_1 \cdot n \text{ и}$$
  $$y - z = k_2 \cdot n.$$

  Сложив эти равенства получим

  $$x - z = (k_1 + k_2) \cdot n,$$

  следовательно, отношение $\equiv$ транзитивно.

Это отношение разбивает множество целых чисел на n классов эквивалентности.
$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$;
$[1] = \{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \ldots\}$;
. . . .
$[n - 1] = \{\ldots, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\}$.

Для явного обозначения натурального числа n, фигурирующего в определении отношения $\equiv$, используют обозначение $\equiv \pmod n$ и вместо $x \equiv y$ записывают

$$x \equiv y \pmod n \text{ или } x = y \pmod n.$$

$$\mathbb{Z}/_{x \equiv y \pmod n} = \{[0], [1], \ldots, [n - 1]\}$$

Теорема. Пусть даны целые числа x, y, u, v и $n \geqslant 1$, причем

$$x \equiv u \pmod{n} \text{ и } y \equiv v \pmod{n}.$$

Тогда

$$x + y \equiv u + v \pmod{n} \text{ и } x \cdot y \equiv u \cdot v \pmod{n}.$$

Иными словами, отношение $\equiv \pmod{n}$ есть конгруэнция алгебры целых чисел с операциями сложения и умножения.

Доказательство.

$$\begin{aligned} x \equiv u \pmod{n} &\leftrightarrow x - u = k_1 \cdot n, \\ y \equiv v \pmod{n} &\leftrightarrow y - v = k_2 \cdot n \end{aligned}$$

для некоторых целых чисел k_1, k_2.

Тогда, во-первых,

$$\begin{aligned} (x - u) + (y - v) &= k_1 \cdot n + k_2 \cdot n, \\ (x + y) - (u + v) &= (k_1 + k_2) \cdot n, \end{aligned}$$

т.е.

$$x + y \equiv u + v \pmod{n}$$

Во-вторых,

$$\begin{aligned} x &= u + k_1 \cdot n, \\ y &= v + k_2 \cdot n, \end{aligned}$$

и, далее,

$$\begin{aligned} x \cdot y &= (u + k_1 \cdot n)(v + k_2 \cdot n) \\ &= u \cdot v + (k_1 \cdot v + k_2 \cdot u + k_1 \cdot k_2 \cdot n) \cdot n, \end{aligned}$$

т.е.

$$x \cdot y \equiv u \cdot v \pmod{n}$$

Теорема доказана.

Следствие. Пусть даны целые числа $n, m \geqslant 1$ и целые числа

$$x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m,$$

такие что

$$x_1 \equiv y_1 \pmod{n}, \quad x_2 \equiv y_2 \pmod{n}, \quad \ldots, \quad x_m \equiv y_m \pmod{n}.$$

Пусть $p(t_1, t_2, \ldots, t_m)$ есть многочлен от m переменных. Тогда

$$p(x_1, x_2, \ldots, x_m) \equiv p(y_1, y_2, \ldots, y_m) \pmod{n}.$$

Это свойство было замечено индийскими математиками около X в. н.э. Оно применялось для проверки расчетов.

Фактор-множество множества $\mathbb{Z}$ по отношению эквивалентности $\equiv \pmod{n}$ с операциями сложения и умножения обозначается $\mathbb{Z}_n$. Его элементы [0], [1], ..., $[n-1]$ обычно обозначаются как обычные числа $0, 1, \ldots, n-1$.

Ниже для примера приведены таблицы сложения и умножения для $\mathbb{Z}_4$ и $\mathbb{Z}_5$.

Таблица 1: $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Таблица 2: $\mathbb{Z}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Теорема. В каждом множестве $\mathbb{Z}_n$ выполнены следующие тождества (называемые аксиомами коммутативного кольца):

1. $x + (y + z) = (x + y) + z$ для всех x, y, z;
2. $x + y = y + x$ для всех x, y;
3. $x + 0 = x$ для всех x;
4. для каждого x существует y, для которого $x + y = 0$;
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ для всех x, y, z;
6. $x \cdot 1 = 1 \cdot x = x$ для всех x;

7. $x \cdot y = y \cdot x$ для всех x;

8. $x \cdot (y + z) = x \cdot y + x \cdot z$ для всех x, y, z.

Бонус: в кольцах $\mathbb{Z}_p$ можно делить! Для простых чисел p кольцо $\mathbb{Z}_p$ есть поле. Оказывается, для простых чисел p кольца $\mathbb{Z}_p$ удовлетворяют дополнительной аксиоме

9. для каждого $x \neq 0$ существует y, для которого $xy = 1$,

и, таким образом, являются *полями*.

Ниже этот факт описан подробно.

НОД, алгоритм Евклида, множители Безу *Общим делителем* целых чисел x и y называется любое целое число n, которое есть делитель числа x и делитель числа y.

Наибольший общий делитель целых чисел x и y это *натуральное* число n, удовлетворяющее условиям

1. n есть общий делитель чисел x и y,

2. каждый общий делитель чисел x и y есть делитель числа n.

Обозначение: НОД(x, y), $\gcd(x, y)$ или просто (x, y).

НОД(x, y) существует и единствен, если хотя бы одно из чисел x, y отлично от нуля. При этом НОД(x, y) есть наибольший (в смысле естественного порядка) из общих делителей чисел x и y.

Наибольший общий делитель можно вычислять, минуя разложение этих чисел на простые множители (алгоритм Евклида).

Описание алгоритма Евклида. Пусть даны натуральные числа x и y, не равные одновременно нулю. Без ограничения общности будем считать, что $x \geqslant y$.

Определим максимально длинную последовательность неотрицательных чисел

$$r_0, r_1, \ldots, r_i, \ldots$$

так, что

- $r_0 = x$,
- $r_1 = y$,

- если $r_i \neq 0$, то r_{i+1} есть остаток от деления r_{i-1} на r_i; иначе последовательность обрывается на i-ом члене.

$$
\begin{aligned}
x &= y \cdot q_0 + r_1 \\
y &= r_1 \cdot q_1 + r_2 \\
&\dots \\
r_{i-2} &= r_{i-1} \cdot q_{i-1} + r_i \\
&\dots
\end{aligned}
$$

Тогда

$$r_0 > r_1 > \ldots > r_i > \ldots$$

Значит, существует номер n, для которого

$$r_{n+1} = 0.$$

Таким образом, последовательность равенств конечна и заканчивается так:

$$
\begin{aligned}
r_{n-2} &= r_{n-1} q_{n-1} + r_n \\
r_{n-1} &= r_n q_n + 0
\end{aligned}
$$

Утверждение.

$$\text{НОД}(x, y) = r_n$$

Доказательство.

1. Если $a = bq + r$, то $\text{НОД}(a, b) = \text{НОД}(b, r)$
2. Поэтому

$$\text{НОД}(x, y) = \text{НОД}(y, r_2) = \ldots = \text{НОД}(r_n, 0) = r_n.$$

Пример. Найти $\text{НОД}(4158, 1056)$.

Решение и ответ.

$$
\begin{aligned}
4158 &= 3 \cdot 1056 + 990 \\
1056 &= 1 \cdot 990 + 66 \\
990 &= 15 \cdot 66 + 0.
\end{aligned}
$$

$\text{НОД}(4158, 1056) = \text{НОД}(1056, 990) = \text{НОД}(990, 66) = \text{НОД}(66, 0) = 66.$

Целые числа x и y называются *взаимно простыми*, если

$$\text{НОД}(x, y) = 1.$$

Теорема. Если число d есть наибольший общий делитель целых чисел x и y, то существуют такие целые числа u и v, что

$$ux + vy = d$$

Следствие. Если целые числа x и y взаимно просты, то существуют такие целые числа u и v, что

$$ux + vy = 1$$

Числа u и v называются *множителями* (или *коэффициентами*) *Безу.*

Доказательство использует алгоритм Евклида *в обратную сторону* и дает практический алгоритм нахождения множителей Безу. Это будет показано на примере (общий случай выглядит практически так же).

Пример. Найти какие-либо множители Безу для чисел 81 и 26.

- Находим НОД$(81, 26)$ с помощью алгоритма Евклида

$$\begin{aligned}
&\underline{\mathbf{81}} = 3 \cdot \underline{\mathbf{26}} + \underline{3} \\
&\underline{\mathbf{26}} = 8 \cdot \underline{3} + \underline{2} \\
&\underline{3} = 1 \cdot \underline{2} + \underline{1} \\
&\underline{2} = 2 \cdot \underline{1} + 0
\end{aligned}$$

  НОД$(81, 26) = 1$.

- Используя протокол выполнения алгоритма, получаем цепочку равенств

$$\begin{aligned}
&\underline{1} = \underline{3} - 1 \cdot \underline{2} = \\
&\underline{3} - 1 \cdot (\underline{\mathbf{26}} - 8 \cdot \underline{3}) = 9 \cdot \underline{3} - 1 \cdot \underline{\mathbf{26}} = \\
&9 \cdot (\underline{\mathbf{81}} - 3 \cdot \underline{\mathbf{26}}) - 1 \cdot \underline{\mathbf{26}} = \\
&9 \cdot \underline{\mathbf{81}} - 28 \cdot \underline{\mathbf{26}}
\end{aligned}$$

  Множители Безу: 9 и -28.

Теорема. Элемент m кольца $\mathbb{Z}_n$ обратим тогда и только тогда, когда

$$\text{НОД}(m, n) = 1$$

Доказательство. Пусть НОД$(m, n) = d \neq 1$. Тогда для некоторых натуральных чисел a, b имеем

$$m = ad \text{ и } n = bd,$$

откуда

$$mb = adb = an = 0$$

в кольце $\mathbb{Z}_n$. Значит, элемент m есть делитель нуля, и поэтому необратим.

С другой стороны, если

$$\text{НОД}(m, n) = 1,$$

то по теорема о линейном представлении НОД для некоторых целых чисел u, v имеем

$$um + vn = 1,$$

откуда в кольце $\mathbb{Z}_n$

$$um = 1.$$

Теорема доказана.

Следствие. Если p-простое, то $\mathbb{Z}_p$ – поле.

5 Задачи

1. Проверить свойства (всюду определенность, функциональность, сюръективность, инъективность) соответствия R из множества X в множество Y. Ответ обосновать.

   (a) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = \{(1, 4), (1, 5), (1, 6)\}$,

   (b) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = \{(1, 6), (2, 5), (3, 4)\}$,

   (c) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = \{(1, 4), (2, 4), (3, 4)\}$,

   (d) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = \{(1, 4), (2, 5)\}$,

   (e) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = X \times Y$,

   (f) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $R = \varnothing$,

   (g) $X = \mathbb{R}$, $Y = \mathbb{N}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{N} : y < x\}$.

   (h) $X = \mathbb{R}$, $Y = \mathscr{P}(\mathbb{N})$,

   $$R = \{(x, y) \in \mathbb{R} \times \mathscr{P}(\mathbb{N}) : (\forall z \in y)\, z < x\},$$

   (i) X и Y есть множество всех людей, когда-либо живших на свете,

   $$R = \{(x, y) \in X \times Y : x \text{ – сын или дочь } y\}.$$

   (j) X и Y есть множество всех людей, когда-либо живших на свете,

   $$R = \{(x, y) \in X \times Y : y \text{ – мать } x\}.$$

   (k) X есть множество всех квадратов на плоскости, Y есть множество всех прямоугольников на плоскости,

   $$x\, R\, y \leftrightarrow \text{площади } x \text{ и } y \text{ равны.}$$

2. Проверить свойства (сюръективность, инъективность) функции $f : X \to Y$. Ответ обосновать.

   (a) $X = \{1, 2, 3\}$, $Y = \{4, 5, 6\}$, $f(x) = x + 3$,

   (b) $X = \{-1, 0, 1\}$, $Y = \{1, 2, 3\}$, $f(x) = x^2 + 1$,

   (c) $X = \{0, 1, 2, 3\}$, $Y = \{1, 2, 3\}$, $f(x) = \min\{x + 1, 3\}$,

   (d) $X = \{0, 1, 2\}$, $Y = \{0, 1, 2, 3, 4\}$, $f(x) = x^2$,

   (e) $X = Y = \mathbb{R}$, $f(x) = x^2$,

   (f) $X = Y = \mathbb{R}$, $f(x) = x^3$,

   (g) $X = Y = \{x \in \mathbb{R} : x \geqslant 0\}$, $f(x) = x^2$,

   (h) $X = Y = \{0, 1, 2, 3, 4, 5, 6\}$, $f(x) =$ остаток от деления $3x$ на 5,

   (i) $X = \mathscr{P}(\{a, b, c, d\})$, $Y = \mathscr{P}(\{b, c, d, e\})$, $f(x) = (x \cup \{e\}) \setminus \{a\}$,

(j) X есть множество всех треугольников на плоскости, Y есть множество всех окружностей на плоскости, $f(x) =$ окружность, описанная вокруг треугольника x

(k) X есть множество всех кругов на плоскости, $Y = \{x \in \mathbb{R} : x > 0\}$, $f(x) =$ площадь круга x,

(l) X – множество всех студентов Университета, $Y = \mathbb{N}$, $f(x) =$ номер студенческого билета студен

(m) $X = Y = \mathbb{R}^2$, $f(x, y) = (3x - 2y, x + y)$,

(n) $X = Y = \mathbb{R}^3$, $f(x, y, z) = (2x + y + z, x + 3y + z, 3x + 4y + 2z)$,

(o) $X = \mathbb{R}^2$, $Y = \mathbb{R}^3$, $f(x, y) = (x + 2y, 3x - y, 4x + y)$,

(p) $X = \mathbb{R}^3$, $Y = \mathbb{R}^2$, $f(x, y, z) = (x - y + z, 2x + y + z)$,

(q) $X = \mathbb{R}^2$, $Y = \mathbb{R}$, $f(x, y) = x^3 + 5xy$.

3. Доказать, что если соответствие P функционально, то

$$P^{-1}(A \cap B) = P^{-1}(A) \cap P^{-1}(B).$$

4. Доказать, что для любых множеств X, Y, Z и соответствий P из множества X в множество Y и R из множества Y в множество Z

   (a) если соответствия P и R всюду определенные, то и соответствие $P \circ R$ всюду определенное,

   (b) если соответствия P и R функциональные, то и соответствие $P \circ R$ функциональное,

   (c) если соответствия P и R инъективные, то и соответствие $P \circ R$ инъективное,

   (d) если соответствия P и R сюръективные, то и соответствие $P \circ R$ сюръективное,

   (e) соответствие P сюръективное тогда и только тогда, когда соответствие P^{-1} всюду определенное,

   (f) соответствие P инъективное тогда и только тогда, когда соответствие P^{-1} функциональное.

5. Доказать, что для любой функции $f : X \to Y$ обратное соответствие является функцией тогда и только тогда, когда f биекция.

6. Описать транзитивное замыкание P^* бинарного отношения P на множестве X.

   (a) $X = \mathbb{N}$, $P = \{(x, y) \in \mathbb{N}^2 : x + 1 = y\}$,

   (b) $X = \mathbb{N}$, $P = \{(x, y) \in \mathbb{N}^2 : x + 2 = y\}$,

   (c) $X = \mathbb{N}$, $P = \{(x, y) \in \mathbb{N}^2 : x \neq y\}$,

   (d) X есть множество всех людей, когда либо живших на свете, $P = \{(x, y) \in X^2 : y$ есть сын или дочь $x\}$,

(e) X есть множество всех людей, когда либо живших на свете, $P = \{(x, y) \in X^2 : y$ есть брат или сестра $x\}$,

(f) $X = \mathbb{N}$, $P = \leqslant$,

(g) X есть множество $\mathscr{P}_2(U)$ всех двухэлементных подмножеств множества $U = \{0, 1, 2, 3, 4, 5\}$,

$$x\,P\,y \leftrightarrow \text{ пересечение } x \cap y \text{ содержит ровно один элемент.}$$

7. Проверить свойства (рефлексивность, иррефлексивность, симметричность, асимметричность, антисимметричность, полнота, связность, транзитивность) бинарного отношения R на множестве X. Указать, является ли R отношением строгого/нестрогого частичного/линейного порядка, отношением эквивалентности. Для отношений эквивалентности описать множество соответствующее разбиение на классы эквивалентности. Ответ обосновать.

(a) $X = \{1, 2, 3\}$; $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$,

(b) $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$; $x\,R\,y \leftrightarrow x$ делится на y,

(c) $X = \mathbb{Z}$, $x\,R\,y \leftrightarrow x - y$ делится на 5,

(d) $X = \mathbb{N}$, $x\,R\,y \leftrightarrow x + 3 \leqslant y$,

(e) $X = \mathbb{N}$, $x\,R\,y \leftrightarrow x + y = 5$,

(f) $X = \mathbb{N}$, $x\,R\,y \leftrightarrow x + y = 10$,

(g) $X = \mathbb{N} \times \mathbb{N}$; $(x, y)\,R\,(x', y') \leftrightarrow x + y = x' + y'$,

(h) $X = \mathscr{P}(\mathbb{N})$, $R = \subseteq$,

(i) $X = \mathbb{N} \times \mathbb{N}$, $(x, y)\,R\,(x', y') \leftrightarrow x + y' = x' + y$,

(j) $X = \mathbb{Z} \times \mathbb{Z}$, $(x, y)\,R\,(x', y') \leftrightarrow xy' = x'y$,

(k) $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$; $(x, y)\,R\,(x', y') \leftrightarrow xy' = x'y$,

(l) X есть множество всех прямых на плоскости, $l_1\,R\,l_2 \leftrightarrow l_1$ параллельна l_2,

(m) X есть множество всех треугольников на плоскости, $\triangle_1\,R\,\triangle_2 \leftrightarrow \triangle_1$ и $\triangle_2$ имеют по крайне мер

(n) X есть множество действительных матриц размера 2×2, $A\,R\,B \leftrightarrow$ существует невырожденная действительная матрица C размера 2×2, для которой $B = CAC^{-1}$,

(o) X есть множество всех дифференцируемых функций $f : \mathbb{R} \to \mathbb{R}$, $f\,R\,g \leftrightarrow f'(0) = g'(0)$,

(p) X множество всех людей, когда либо живших на свете, $u\,R\,v \leftrightarrow$ u и v имеют по крайней мере одного общего дедушку или по крайней мере одну общую бабушку.

8. Построить бинарное отношение на множестве $\{0, 1, 2\}$, которое

(a) рефлексивно, симметрично, но не транзитивно,

(b) рефлексивно, транзитивно, но не симметрично,

(c) симметрично, транзитивно, но не рефлексивно.

9. Доказать, что для любых множеств X, Y функции $f : X \to Y$ бинарное отношение
$$R = \{(x, y) : f(x) = f(y)\}$$
на множестве X есть отношение эквивалентности.

10. Вычислите:

a. $13 + 17$ в кольце $\mathbb{Z}_{20}$;

b. $9 \cdot 5$ в кольце $\mathbb{Z}_{14}$;

c. -3 в кольце $\mathbb{Z}_5$;

d. $4 \cdot (6 + 8) + 3 \cdot 7$ в кольце $\mathbb{Z}_{10}$;

e. $4 \cdot 9 - 5 \cdot 8$ в кольце $\mathbb{Z}_{11}$;

f. 3^5 в кольце $\mathbb{Z}_5$;

g. 17^{25} в кольце $\mathbb{Z}_{18}$.

Ответом должно быть целое неотрицательное число k, не превосходящее $n - 1$ – с формальной точки зрения это класс эквивалентности числа k по отношению равенства по модулю n.

Для энтузиастов

11. Найдите $\gcd(4321, 10556)$, используя алгоритм Евклида.

12. Используя результат предыдущей задачи, найдите какие-нибудь множители Безу для чисел 4321 и 10556.

13. Вычислите:

(a) 5^{-1} в поле $\mathbb{Z}_{13}$;

(b) 4^{-1} в кольце $\mathbb{Z}_9$;

(c) 3^{-3} в поле $\mathbb{Z}_7$.

14. Решите уравнение:

(a) $4x = 7$ в поле $\mathbb{Z}_{11}$;

(b) $5x = 4$ в кольце $\mathbb{Z}_{12}$.

15. Докажите, что, если $\gcd(n, m) = 1$, то
$$x \equiv y \pmod{nm}$$
тогда и только тогда, когда
$$\begin{cases} x \equiv y \pmod{n} \\ x \equiv y \pmod{m} \end{cases}$$

16. Используя результат предыдущей задачи, решите уравнение

    (a) $6x = 5$ в кольце $\mathbb{Z}_{20}$;

    (b) $3x = 15$ в кольце $\mathbb{Z}_{21}$.

6 Ответы и указания

1. Указаны только те свойства, которыми функция обладает. Если функция не обладает никаким из требуемых свойств, ответ в списке отсутствует. 1a сюръективно, 1b биективно, 1c функционально и всюду определено (R – функция), 1d функционально, но не всюду определено (R – частичная функция), 1e сюръективно и всюду определено, 1f инъективно и функционально, 1g сюръективно, 1h всюду определенная функция, 1i всюду определенное, 1j всюду определенная функция, 1k всюду определенное и сюръективное. 2. В основном указаны только те свойства, которыми соответствие обладает. 2a биекция, 2c сюръекция, 2d инъекция, 2f биекция, 2g биекция, 2h биекция, 2j сюръекция, 2k сюръекция, 2l инъекция, 2m биекция, 2o инъекция, 2p сюръекция, 2q сюръекция. 3 Указание: функциональность используется при доказательстве включения справа налево. 6. 6a $<$, 6b $\{(x, y) \in \mathbb{N}^2 : x < y \wedge y - x$ делится на два$\}$, 6c $\mathbb{N}^2$, 6d $\{(x, y) \in X^2 :$ y потомок $x\}$, 6e $\{(x, y) \in X^2 : x = y$ или y есть брат или сестра $x\}$, 6f $\leqslant$, 6g $\mathscr{P}_2(U) \times \mathscr{P}_2(U)$. 7. Указаны только основные свойства. 7a отношение эквивалентности, 7b отношение нестрогого частичного порядка, 7c отношение эквивалентности, 7d отношение строго частичного порядка, 7e иррефлексивное и симметричное, 7f симметричное, 7g рефлексивное и симметричное, 7h отношение нестрого частичного порядка, 7i отношение эквивалентности, 7j рефлексивное и симметричное, 7k отношение эквивалентности, 7l иррефлексивное и симметричное, 7m рефлексивное и симметричное, 7n отношение эквивалентности, 7o отношение эквивалентности, 7i рефлексивное и симметричное. 8. Например, 8a. $\{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}$, 8b. $\{(a, a), (b, b), (c, c), (a, b)\}$, 8c. $\varnothing$.